QUALYS
SECURITY ON-DEMAND

ADVISORY

Qualys Security Advisory \ January 13, 2004

# H.323 Implementation Vulnerabilities on Multiple Platforms

## ADVISORY OVERVIEW

January 13, 2004 – Qualys™ Vulnerability R&D Lab today released new vulnerability signatures in the QualysGuard® Web Service to protect enterprises against vulnerabilities in multiple vendors' implementations of the H.323 multimedia telephony protocol. Customers can immediately audit their networks for these vulnerabilities by accessing their QualysGuard subscription.

## VULNERABILITY DETAILS

A vulnerability was announced today in the implementation of the H.323 protocol in products from multiple vendors. An attacker can potentially exploit this vulnerability to produce results ranging from a denial of service (DoS) condition to remote compromise of the vulnerable system.

The H.323 protocol is used in numerous telephony and multimedia products in IP networks. It may be used in hardware products supporting multimedia conferencing as well as various operating systems. The H.225 subcomponent of the H.323 protocol was found to have multiple vulnerabilities in various vendor implementations of the protocol. H.225 is most commonly used as a component of Voice over IP (VoIP).

The vulnerability affects VoIP, videoconferencing, and telecommunications products from a number of vendors. Among the vendors known to be vulnerable:

1. Microsoft® ISA Server™ 2000 (MS04-001) (CAN-2003-0819) is vulnerable to a buffer overflow in the Microsoft Firewall Service that could allow a remote attacker to execute malicious code. For additional information about affected Microsoft platforms and available patches, please visit the Microsoft Security Bulletin at: http://www.microsoft.com/technet/security/bulletin/ms04-001.asp

2. Cisco® IOS Firewall and multiple non-IOS products are susceptible to a DoS condition caused by parsing malformed H.323 packets. For additional information about

© Qualys, Inc. All rights Reserved

affected platforms and available patches, please visit the Cisco Advisory at: http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

Users of other H.323-based VoIP, videoconferencing, and telecommunications equipment should contact their vendors for information about potential vulnerabilities and availability of updates.

For additional information concerning the H.323 protocol vulnerabilities, please visit the Carnegie Mellon CERT® Coordination Center knowledge base at: http://www.kb.cert.org/vuls/id/749342

## HOW TO PROTECT YOUR NETWORK

Checks for the H.323 protocol vulnerability are already available in the QualysGuard vulnerability management platform. A default scan will detect these issues. In addition QualysGuard users can perform a selective scan for these specific vulnerabilities using the following checks:

- "Microsoft Internet Security and Acceleration Server 2000 H.323 Filter Buffer Overflow Vulnerability" (CAN-2003-0819) (MS04-001)
  - Qualys ID: 90088
  - Limit the scan to TCP ports 139 and 445
  - Windows login required

- "Multiple Vendor H.323 Protocol Implementation Vulnerabilities"
  - Qualys ID: 38246
  - Limit the scan to TCP port 1720
  - This signature generates a Possible Threat

## TECHNICAL SUPPORT

For more information, customers can contact Qualys Technical Support directly at support@qualys.com or 1-866-801-6161.

## ABOUT QUALYSGUARD

QualysGuard is an on-demand security audit service delivered over the web that enables organizations to effectively manage their vulnerabilities and maintain control over their network security with centralized reports, verified remedies, and full remediation workflow capabilities with trouble tickets. QualysGuard provides comprehensive reports on vulnerabilities including severity levels, time to fix estimates and impact on business, plus trend analysis on security issues. By continuously and proactively monitoring all network access points, QualysGuard dramatically reduces security managers' time researching, scanning and fixing network exposures and enables companies to eliminate network vulnerabilities before they can be exploited.

Access for QualysGuard customers: https://qualysguard.qualys.com

Free trial of QualysGuard service: http://www.qualys.com/forms/maintrial.html

© Qualys, Inc. All rights Reserved